Making the difference

Information Governance Policy

INFORMATION GOVERNANCE POLICY

INTERNET, EMAIL, MOBILE PHONE & SOCIAL MEDIA INFORMATION

The Charity has invested in the necessary resources to ensure that it is able to make the most of the advantages offered by modern electronic communication technology. We are committed to maintaining and updating this capability. The Telephone system, Internet, Intranet and e-mail facilities may only be used for the purposes of the Charity.

This policy and guidelines contain herein are to be regarded as part of the 'Code of Conduct' for all members of staff (See 'Guidance for all Staff' document). Failure to observe the procedures it contains, and any amendments or addition to these guidelines that may be published from time to time, may be regarded as misconduct or gross misconduct and will be dealt with under the charities Code of Disciplinary Procedure.

Use of the Internet

- The Charity's website may be found at **www.vranchhouse.org** and is to be set on all computers as the default site for MS Edge and Chrome browsers alike. No other internet browser but MS Edge and Chrome may be used. Members of staff are encouraged to visit the Charity's website regularly as the site is rewritten every year and updated throughout the year roughly every two weeks. Suggestions for any additions or improvements to the website should be sent to the Chief Executive.
- All members of staff may access other websites relevant to their work. No orders may be made by any member of staff unless specifically authorised to do so by the Chief Executive. No programs (software) may be downloaded or installed on a work computer without the permission of the Chief Executive. The unauthorised downloading of copyright material and the copying or distribution of copyright material without authority will be regarded as Gross Misconduct.
- No member of staff may access any website whatsoever which is not related to the proper business of the Charity. Accessing any websites or material which might be regarded 'inappropriate' under the following headings will be regarded as Gross Misconduct:
    - **Discrimination** – content that is unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010
    - **Drugs / Substance abuse** – content in the promotion or displaying of illegal drugs or harmful substances
    - **Extremism** – any content that that promotes intolerance, violence toward others (including terrorist acts) or extreme ideologies
    - **Malware / hacking** – sites and materials that promote the compromising of computer systems, bypassing security or filtering measures or accessing sites hosting malicious content
    - **Pornography** – any sites that display content of a sexually explicit nature
    - **Piracy and copyright theft** – sites that offer software for copy/distribution of images or other data without consent form the copyright owner
    - **Self-harm** – any content that promotes or displays deliberate self-harm, including suicide and eating disorders
    - **Violence** – content that promotes verbal or physical aggression towards others with the intent to harm or kill
- Our Ubiquiti UniFi internet filter and firewall should prevent 'accidental' accessing of websites promoting content listed above; if any member of staff using our internet server attempts to directly access inappropriate content this will therefore be a deliberate act and considered Gross Misconduct.

- The above list is not exhaustive; if any staff to attempt to access any materials that are later deemed inappropriate by the Chief Executive or Head of Education, such an act may also be regarded as Gross Misconduct.
- The Charity reserves the right to examine any of its computers at any time and employees should be aware that improperly downloaded material is recoverable whether or not it has been deleted.

Use of the Intranet (designated 'CENTRAL_DATAHUB' on the network)

- The Charity operates a Central Information Hub accessible through the intranet (note this is a network NOT connected to the World Wide Web and not accessible from outside Vranch House). Any computer connected to the intranet will have access to data held on the Central Hub. All information placed in shared folders is regarded as confidential to the Charity and may not, under any circumstances, be passed to any individual not employed by the Charity.
- No data generated on any device connected to the intranet can be saved on the local device; it MUST be saved to the Central Hub. This is for three reasons; 1. The Central Hub is a protected data device and is automatically backed-up to a device on the intranet but outside the main Vranch House building. **2.** There should only be one copy of a record. Keeping a local copy could lead to confusion as to what is the latest version of any document. **3.** Information generated by employees belongs to Vranch House and the Charity must have access to it.

Use of E Mail

- Email may normally only be used to communicate internally with colleagues on business matters and externally to clients and suppliers. Urgent or important messages to family and friends are permitted but must be of a serious nature (the judgement here is to whether or not the communication is important). Time misspent in idle correspondence may be regarded as misconduct. The mailing of jokes, comments and rumours or of any judgement that might be regarded as libellous is not permitted and any message containing sexually explicit or otherwise inappropriate material (see above), whether sent internally or externally will be regarded as Gross Misconduct. The Charity might well invoke the Code of Disciplinary Procedure in the event that banned material is sent but employees should note that the legal responsibility for contravening these guidelines will remain theirs individually as will any claim or liability arising from the sending of such material.
- No email which might be regarded as harassing, insulting or bullying may be sent. Complaints about another department's or individual's performance or service should be made according to the Charity's complaints procedure i.e. initially by verbal or written report to the Department Head.
- The Charity recognises that it is not always possible to control incoming mail. Any employee receiving unwarranted mail containing material which is banned under these guidelines should delete that message. Repeated attempts should be reported to the Chief Executive.
- All email sent from any Charity computer must contain the signature authorised by and available from the Chief Executive. This signature must be included on both original messages and replies. Failure to use this signature will be construed as Misconduct.
- MS Outlook, Eclipse webmail and nhs.net are the only email software programs to be used on Charity computers and the only accounts through which email may be sent are the accounts set up by the Charity.
- All employees using email must be aware that electronic messages, although quick and convenient, should still reflect the image, professionalism and courtesy of this Charity. Do not so compress the message that the normal courtesies are left out and do remember to use F7 in MS Outlook to spell-check before sending the message.

- All emails are to be filed. It is the responsibility of any employee using email to ensure that important messages, whether sent or received, are printed and filed as a "hard copy". Only unsolicited mail or mail contravening these guidelines is authorised for deletion.
- The Charity reserves the right to monitor incoming and outgoing emails.

Portable Data Storage

- Only Flash Drives (also referred to as USB 'sticks' or 'pen drives') provided by the Charity are to be used on-site at Vranch House.
- Data copied to a flash drive is to be used ONLY to move data between computers at Vranch House and the copying without permission of any program or file or any other data held on a computer at Vranch House to a private computer off-site is a disciplinary offence.
- Flash Drives are NOT to be used as a back-up device (they are too easily lost and the danger of compromised confidential data is too great). If you need a back-up device other than the CD or DVD drive in your computer, speak to the Chief Executive.
- If you need to take data off-site you will need the express permission of the Chief Executive who will keep a register of those so authorised.
- Remember that you can use the network to move data from one computer to another within Vranch House without emailing it or using a Flash Drive.
- The hard drive of any computer leaving service at Vranch House will be destroyed.

Data Transmission

You may need to use email to send documents or other data as attachments. In every case where this information relates to an individual it is to be sent via encrypted email such as Egress or the NHS email client. Where staff do not have access to such software, any shared files should be password protected; for example in MS Word:

- Use issued password and email it to the addressee with the message that the password will be needed to open a document you will be sending separately.
- Open the document in MS Word and Select Tools/Options/Security.
- At "Password to Open" enter your chosen password.
- Attach the document to your email message and send.

Personal information should not be sent in an open email but ONLY in a password protected attachment and, obviously, never include the password with the message that accompanies the protected document.

As the security of "personnel in confidence" information is a high priority any breach of this policy could be treated as a disciplinary offence.

Personal Contact Information

In essence the following is **NOT PERMITTED (i.e. an infraction of this policy would be regarded as Gross Misconduct and make an employee liable to instant dismissal)**:

- Giving out a private email address or telephone number to a school pupil or outpatient.
- Engaging in web-based communication AT ANY TIME with pupils or outpatients, or members of their families, using software technologies like "Twitter", "MSN" or "Facebook".
- Communication with pupils, outpatients and families must at all times be on professional matters only, on headed paper or by email carrying the approved Vranch House signature. It is a disciplinary offence to permit or encourage a professional relationship to develop into a private one.
- If at any time you are concerned that a relationship is being pushed across the professional boundary into private territory, you should immediately share your concerns with your

departmental manager (one of the three members of the Senior Management Team). This will protect you from any later claims of an inappropriate relationship.

Use of Personal Mobile Phones at Work outside Offices

Staff must not under any circumstances or for any reason use a mobile phone while at work OUTSIDE OFFICES. Mobile phones should be switched off during working hours but may be used in the grounds or the Staff Room during the lunch hour. If you need to be contacted then the main switchboard number (01392 468333) should be given as the contact phone number.

General

- Electronic communications systems are convenient, can amplify the capacity to get work done and can be used for the effective acquisition and distribution of information. Remember that the downside is that your computer is connected to the world. The network is protected by a firewall but it is your responsibility to ensure that your anti-virus software is running **whenever you connect to the net.**
- It is good practice to treat electronic communications as you would treat written correspondence. You would throw junk mail away, you would expect to be treated with dignity and respect by people writing to you and you would act if any letter you received contained threats, libellous or obscene material or which compromised your own privacy.
- Remember that everything you write carries the good name of this Charity with it every time you press the "Send" button!
- Information about individuals should always be treated as confidential and password protected. Be very careful to take care of any media on which information is stored.
- If you have any questions at all about these guidelines or about your day to day use of the system, do not hesitate to ask the Chief Executive.
-

WRITTEN, PRINTED& DIGITAL RECORDS

General

Where electronic data or a record of any kind is taken in writing or print and the resulting document is retained;

- The information should only be retained because it is relevant to the clinical treatment of a pupil or outpatient, to the provision of educational services to a school pupil or to the legal management of the business.
- Retained documents must be in a format approved and promulgated by the relevant Head of Service (the Head of Therapies or the Head of Education).
- All printed documents must be held securely in locked cabinets.
- All digital information is to be held on the Central Data Hub
- Access to retained files must be only on a need-to-know basis. Employees accessing records which they have no professional need to see could be liable to disciplinary action.

Retention Times

Records should only be retained if;

- The information the record contains remains relevant; or,
- The record must be retained for legal reasons;
  - Medical and School records until the individual is 25 years of age.
  - Employer's Liability Certificates for 30 years.
  - Business records for 20 years.
  - Employees' Records for 20 years.

The General Data Protection Regulation (GDPR)
The keeping and management of Business, Personal and Personnel Records is governed by the General Data Protection Regulation (GDPR) of 2018. The regulation applies if the data controller (an organisation that collects data from EU residents), or processor (an organisation that processes data on behalf of a data controller like cloud service providers), or the data subject (person) is based in the EU.

For the purpose of the GDPR – "personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address".

The governing principles are that Personal Information must be;
a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Subject's Rights.
The GDPR provides the subject with the following individual rights with regard to his or her personal information:

- The right to be informed about the collection and use of personal data.
- The right of access to their personal data and supplementary information.
- The right to have inaccurate personal data rectified or completed if it is incomplete.
- The right to erasure (to be forgotten) in certain circumstances.
- The right to restrict processing in certain circumstances.
- The right to data portability, which allows the subject to obtain and reuse his/her personal data for his/her own purposes across different services.
- The right to object to processing in certain circumstances.
- Rights in relation to automated decision making and profiling.
- The right to withdraw consent (where relevant).

- The right to complain to the Information Commissioner.

The Stated Purpose

The stated purpose for retaining personal information at Vranch House is that only information necessary for the following business activities should be retained and is held in accordance with our Privacy Statement:

- Information essential to the provision of educational and clinical services to school pupils and outpatients.
- Information necessary for paying an employee correctly which includes information for ensuring company and employee contributions to relevant pension schemes are made on time.
- Information relating to the attendance record, the next-of-kin, any special employment conditions (relating to health needs, the need to worship, or any other factor the employee has requested the employer to note in order to facilitate the employment).
- Information relating to any disciplinary action taken in redress of an employment difficulty (such records to be expunged when the employee is no longer employed unless the action was consequent upon a breach of common law).
- Information relating to Continuous Professional Development.
- Contractual information involving the employer and the employee jointly in any document signed by both parties.

Destruction of Retained Documents

When any document is considered redundant, has reached its terminal date or no longer needs to be held for the Stated Purpose then it is to be destroyed. The mandated method for destruction is by confidential burn-bags. The files selected for destruction are placed in sealed burn-bags and then burned by a contractor certified for the secure destruction of confidential records.

Disclosure of Retained Documents

Retained documents may be disclosed to;

- Any partner agency with whom we work with, on a contractual basis, to deliver our services who without disclosure of such documents would be unable to provide such services and comply with their statutory obligations.
- Any employee who wishes to see his or her Personnel File.
- Any legal authority requesting sight of a record for a legal action provided the request is deemed by the Chief Executive to be correct but such a disclosure can only include information **over which Vranch House has copyright**.
- Any parent or guardian wishing to see a medical or school record.
- The Police in pursuance of a criminal investigation either by request which is acceded to or in accordance with the terms of a Search Warrant.

The Vranch House nominated GDPR officer

Whilst every individual who handles or processes data must comply with the law, Vranch House believes it is a good idea to have one person who oversees the data processing to ensure that they are meeting all security obligations.

Our GDPR officer is responsible for ensuring the organisation's compliance with the General Date Protection Regulations. This responsibility is delegated by the Chief Executive.

Responsibilities of our GDPR officer:

- Be the nominated officer on the GDPR Register.
- Develop and implement the organisation's Information Governance Policy.
- Create 'best practice' guidance for data processors, preferably in written form for future reference.
- Train and advise staff on the provisions of the General Data Protection Regulations.

Kate Moss - Chief Executive
Sept 2021